1. Volunerabilities

By definition Security vulnerabilities are defined as weaknesses in technology, software, or operational practices that can be exploited by threats, leading to potential risks such as unauthorized access or information leakage [1]. These vulnerabilities can tak on various forms and in this paper I will be focusing on open source tools designed for finding flaws in networks and web applications.

2. Classification

Security vulnerability can be categorized into four categories those being software vulnerabilities, hardware vulnerabilities, configuration and operational vulnerabilities, and physical and personnel vulnerabilities [1]. Each of these catogiries has many sub categories and here I will be focusing only on network and web based software vulnerabilities. Classification of Common Vulnerabilities and Exposures(CVE) is provided by NVD which is using Common Weakness Enumeration(CWE) classification mechanism that differentiates CVEs by the type of vulnerability they represent. This classification distributes CVEs into a hierarchical structure CWE on higher level provide overview of vulnerability type and can have many subtypes. CWE are classified based on their nature and effect.

Main types of CVE this paper will be focusing on will be

- CWE-352: Cross-Site Request Forgery
- CWE-425: Direct Request (‘Forced Browsing’)
- CWE-668: Exposure of Resource to Wrong Sphere
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- CWE-552: Files or Directories Accessible to External Parties
- CWE-287: Improper Authentication
- CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)
- CWE-307: Improper Restriction of Excessive Authentication Attempts
- CWE-444: Inconsistent Interpretation of HTTP Requests (‘HTTP Request/Response Smuggling’)
- CWE-613: Insufficient Session Expiration
- CWE-918: Server-Side Request Forgery (SSRF)
- CWE-521: Weak Password Requirements

All of which you can read more about on official nvd website.

3. Characteristics

3.1. Cross-site request forgery(csrf)

is a vulnerability that takes advantage of web application in which target is currently authenticated and by gaining the targets authentication token the attacker proceed to make actions as if they were the target. This attack can lead to anything from sending messages on victims behalf up to transfering money. In worst cases entire web applications can be compromised if user has high level of auhtorization.

3.2. CWE-425: Direct Request (‘Forced Browsing’)

Direct Request or more commonly known as Forced browsing is a type of vulnerability that allows resctricted conten be accessed by unathorized users. This can be achieved by searching trough bruteforce for unlinked content on the server such as directories, temporary files or configuration files. As these files can contain sensitive information, prevention against this attack is vital. These attacks can be done both manually if too much context is given to user or trough automated tools such as Nitko. Nikto, open source too used for scanning vulnerabilities is capable of searching trough most common directories based on it’s database and report the results to user. Example: with

the use of nikto, an example website “www.exampl.com” would be scanned for most common directories like example.com/users , example.com/logs, example.com/images and more.

3.3. CWE-668: Exposure of Resource to Wrong Sphere

Exposure of Resource to Wrong Sphere vulnerability allows a wrong person to access files meant for someone else. It’s a vulnerability may sound similar to CWE-425 but main difference between these 2 CWEs is that CWE-668 could allow unauthorized person to read sensitive data from database or images from folder not accessible to them due to logical error. CWE-425 however attempts read all vulnerable information from files the serever. For easier understanding you can imagine it as someone accessing groupchat access to group he’s not a part of.

3.4. CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

todo:wtf is the difference between this and 668 ?

3.5. CWE-552: Files or Directories Accessible to External Parties

This CWE is a relatively common mistake for beginners and missconfiguration of a server that allows unathorized user to access files not meant for them. This can affect any type of web server, ftp or similar server and is nearly always caused by missconfigured authorization. Most common way of abusing this missconfiguration is by using chroot() function.

3.6. CWE-287: Improper Authentication

Improper Authentication is quite self explenatory. Even tho it’s not a common vulnerability in this day and age the concept itself is something which needs to be addressed whenever a new security system is being made. Simply put, one needs to make sure that user trying to log in is who they say they are. Example of improper Aithentication would be a website where use logs in with username only.

3.7. CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

Cross-site Scripting is a practice in which attacker injects into website a malicious piece of code trough form of a social media post, a message or anything that other user may display. This malicios code when loaded by another client can cause harm in form of sharing private session key causing csrf or perhaps even by collecting sensitive user data. It is up to the developer to analyze and properly neutralize user input so this type attack is not possible.

3.8. CWE-307: Improper Restriction of Excessive Authentication Attempts

Password cracking is to this day a huge topic and one of it’s simplest forms is brute force attack. This type of attack will attempt to try every possible combination of available options to get past authentication system. As inneficient as it might seem, it’s still very effective to this day because numerous systems still use a 4 digit authentication which can theoretically be broken in mere milliseconds. Standard precaution against this vulnerability is a restriction that is put into place which prevents user to login for set time after failing login some number of times.

3.9. CWE-444: Inconsistent Interpretation of HTTP Requests (‘HTTP Request/Response Smuggling’)

This vulnerability has once again to do with inproper configuration. Attacker may use bad configuration of http response length to inject target device with malicious code that is given to client after the original message but pretends to be a part of it. This way even tho the web server deems the message to be safe the program will interprete it as 2 different actions allowing attacker to take unwanted action in the server.

3.10. CWE-613: Insufficient Session Expiration

Insufficient Session Expiration can be abused by anyone listening in on your network.As web browsers put sessions informatino in your cookies, anyone listening on your nework may record this session. A recorded conversation over the network could be later used to access someones account and unwanted actions can be made in place of the user causing potential harm.

3.11. CWE-918: Server-Side Request Forgery (SSRF)

SSRF is an attack which attempts to infiltrate internal network. By deceiving a web server, attacker may force server to send malicious action to devices in internal network therefore bypassing security as it's sent from a trusteddevice. Difference between SSRF and CSRF is that SSRF targets server itself. CSRF is on the other hand targeting user itself and making action on client side.

3.12. CWE-521: Weak Password Requirements

4. Tools For Finding Web Vulnerabilities

applications to describe Dirsearch,w3af,nikto,CloudSploit,Wapiti,Vega,Grabber

5. w3af

w3af includes csrf testing

Bibliography

[1] "Security Vulnerability." [Online]. Available: **https://www.sciencedirect.com/topics/computer-science/security-vulnerability**